DZ CompliancePartner

BAIT 2021

Auszug wesentlicher Handlungsempfehlungen

Neu-Isenburg, 9. September 2021

DZ CompliancePartner GmbH
Wilhelm-Haas-Platz
63263 Neu-Isenburg

info@dz-cp.de
www.dz-cp.de

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken

DZ CompliancePartner

Inhalt **Seite**

1 Überblick wesentlicher Anpassungsbedarfe für den Vorstand

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
1.2 a	Berücksichtigung der ergänzenden Hinweise zur IT-Strategie: • Aussagen zu Abhängigkeiten von Dritten • Ziele der Informationssicherheit • grundlegende Aussagen zur Schulung und Sensibilisierung der Informationssicherheit	Im wesentlichen Umformulierung, jedoch auch Erweiterung auf „wichtige Abhängigkeiten von Dritten“ anstelle „Auslagerungen“ (wie z. B. Zentralbankfunktion, Informationsdienste, Telekommunikationsdienstleistung, Versorgungsleistung etc.). Dies ist in der IT-Strategie entsprechend zu berücksichtigen.	IT-Strategie	Vorstand/Fachabteilung in Abstimmung mit Informations-sicherheitsbeauftragten
1.2 b	Zuordnung der gängigen Standards, an denen sich das Institut orientiert, auf die Bereiche der IT und der Informationssicherheit	Lediglich Konkretisierung, kein Anpassungsbedarf (über textuelle Anpassung in der IT-Strategie) hinaus.	IT-Strategie	Vorstand/Fachabteilung in Abstimmung mit Informations-sicherheitsbeauftragten
1.2 c	Ziele, Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation	Aufnahme der Ziele der Informationssicherheit in die IT-Strategie. Insbesondere sind - sofern noch nicht enthalten - Aussagen zu Schulungen im Bereich der Informationssicherheit zu ergänzen. Ggf. sind daraus aufgrund der Bedeutung auch Maßnahmen / Ziele abzuleiten.	IT-Strategie	Vorstand/Fachabteilung in Abstimmung mit Informations-sicherheitsbeauftragten
1.2 e	Aussagen zum IT-Notfallmanagement unter Berücksichtigung der Informationssicherheitsbelange	Erweiterung des Notfallmanagements gem. AT 7.3 MaRisk zu einem IT-Notfallmanagement (über die zeitkritischen Aktivitäten und Prozesse hinaus) sowie Berücksichtigung von Informationssicherheitsbelangen im Notfallmanagement.	IT-Strategie	Vorstand/Fachabteilung in Abstimmung mit Informations-sicherheitsbeauftragten

2 Überblick wesentlicher Anpassungsbedarfe für die IT-Organisation

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
		Dieses Kapitel ist komplett neu in den BAIT. Diese neuen Anforderungen (insb. Wirksamkeitskontrollen für umgesetzte Informationssicherheitsmaßnahmen in Form von Tests und Übungen - Schwachstellenscans, Penetrationstests, Simulation von Angriffen etc.) sollten seitens der Banken in einer internen Richtlinie fixiert werden. Hierzu sollte auf zu erwartende Muster-Arbeitsanweisungen der Verbände zurück gegriffen werden. Es ist insb. anhand der Verbundinterpretation des BVR bankseitig zu entscheiden, ob dieses Kapitel relevant ist. Bei einer geringen Anzahl von zudem unwesentlicher bankeigen betriebener IT hat dieses Kapitel nach Auffassung der DZ CP eine deutlich geringere Bedeutung als bei Banken, bei denen ein größerer Teil von wesentlicher in bankeigener Verantwortung betriebener IT vorhanden ist.	neue Richtlinie	IT-Organisation in Abstimmung mit Informationssicherheits-beauftragter
	Überprüfung der Implementierung der Informationssicherheitsmaßnahmen und -Prozesse			
	– Überprüfung, dass vorhandene Protokolldaten der Bank zeitnah ausgewertet werden. – Zukünftige Nutzung des Standardangebots der Fiducia & GAD agree21OpSec (Breiteneinsatz ab 2022), ggf. Projekt zur Anbindung bankeigener Systeme			
	– Überprüfung der individuellen IT gemäß Richtlinie über das Testen und Überprüfen von Maßnahmen der Bank (vgl. Nr. 4.8 BAIT) – Überprüfungen mit IT-Dienstleistern vertraglich regeln – Überwachung und Steuerung der durch die Fiducia & GAD vorgenommenen Überprüfungen, Auswertung der quartalsweisen ISM-Reports und Risikoberichte			

DZ CompliancePartner

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
6.2	Überprüfung der Zutrittsrechte zu Räumen	Die in den BAIT aufgenommene Erweiterung auf "Zutrittsrechte zu Räumen" ist bei den Regelungen und Prozessen zum Identitäts- und Rechtemanagement - soweit noch nicht vorhanden - entsprechend zu berücksichtigen. Ebenso sind in der Tz. Tlw. Konkretisierungen von Vorgehensweisen enthalten, hier ist zu überprüfen, ob diese bereits in den bestehenden Regelungen/ Prozesse angemessen berücksichtigt werden.	Berechtigungsmanagement	IT-Organisation
6.4	Überprüfung der zeitnahen oder unverzüglichen Umsetzung der Berechtigungsanträge	In den Erläuterungen wurde eine Begründung für eine zeitnahe Deaktivierung von Berechtigungen angeführt, diese sollte in die Regelungen und Prozesse zum Berechtigungsmanagement übernmommen werden.	Berechtigungsmanagement	IT-Organisation
6.7	Überprüfung des Umgangs mit privilegierten Benutzer- und Zutrittsrechten	Die Anforderung zur Protokollierung / Überwachung der Aktivitäten mit privilegierten Rechten ist nicht neu, stand jedoch bisher "nur" in der Erläuterungen. Durch die Überführung wird die Bedetung hervorgehoben. Es sollte überprüft werden - zusamen mit der "neuen" Definition der privilegierten Zutrittsrechte, ob dies bereits in den bestehenden Regelungen und Prozessen berücksichtigt ist.	Berechtigungsmanagement	IT-Organisation
8.2	Überprüfung, ob eine Übersicht der Komponenten der IT-Beziehung sowie deren Beziehungen zueinander mit den erforderlichen Bestandsangaben geführt wird (insbesondere Ergänzung BAIT-Novelle beachten)	In den Erläuterungen sind neue Bestandsangaben (Eigentümer der Informationssýsteme, Schutzbedarf der IT-Systeme) hinzugekommen. Diese sind nicht grundsätzlich neu, es sollte überprüft werden, ob diese bereits in dem Bestandsverzeichnis der Bank sowie den Regelungen in der Bank enthalten sind.	Softwareeinsatz	IT-Organisation

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
8.6	Überprüfung, dass organisatorische Regelungen zu Standardvorgehensweisen bei Störungen vorhanden sind.	Es ist eine Anforderung neu aufgenommen hinsichtlich Standardvorgehensweisen für Abweichungen vom Regelbetrieb. Dies sollte an sich in der angegebenen Organisationsunterlage bereits enthalten sein, dies sollte jedoch bankseitig überprüft werden. Zudem sollte überprüft werden, ob bereits Kriterien für die Information der zuständigen Aufsichtsbehörde enthalten sind.	Störungs-/Incident-management	IT-Organisation
8.8	Überprüfung der Kontrolltätigkeiten innerhalb der Bank hinsichtlich der Leistungs- und Kapazitätüberwachung.	Neue Anforderung. Sofern eine Erfordernis für die Umsetzung gesehen wird, ist dies entsprechend in den Regelungen / Prozessen darzustellen. Ggf. könnte - insb. bei nur bei wenigen / unwesentlicher eigenbetriebener IT-Systeme - eine Argumentationskette für die Nicht-Notwendigkeit erarbeitet werden.	Softwareeinsatz	IT-Organisation
11.1	Management der Beziehungen mit Zahlungsdienstnutzern	Dieses Kapitel ist komplett neu in die BAIT aufgenommen worden. Diese neuen Anforderungen (insb. direkte Adressierung der Zahlungsdienstnutzer für die Reduzierung von (Betrugs-)Risiken etc.) sollten seitens der Banken in einer internen Richtlinie fixiert werden. Hierzu sollte auf zu erwartende Muster-Arbeitsanweisungen der Verbände zurück gegriffen werden.	Neue Richtlinie	IT-Organisation, Zahlungsverkehr
11.2	Überprüfung, ob der Zahlungsdienstnutzer über sicherheitsrelevante Risiken über einen geeigneten Weg informiert wird	Hier wird insbesondere auf eine Information / Sensibilisierung der Zahlungsdienstnutzer abgestellt. Analoge Regelungen sind seinerzeit mit den MaSI / PSD2 gefordert worden, auf diese kann ggf. zurückgegriffen werden.	Neue Richtlinie	IT-Organisation, Zahlungsverkehr

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
11.3	Überprüfung der dem Zahlungsdienstnutzer angebotenen aktuellen Sicherheitsinformationen.	Hier wird insbesondere auf die Aktualität der Information / Sensibilisierung der Zahlungsdienstnutzer abgestellt. Analoge Regelungen sind seinerzeit mit den MaSI / PSD2 gefordert worden, auf diese kann ggf. zurückgegriffen werden.	Neue Richtlinie	IT-Organisation, Zahlungsverkehr
11.4	Überprüfung der dem Zahlungsdienstnutzer angebotenen Möglichkeiten zur Deaktivierung von Zahlungsfunktionalitäten	Das ist eine eher technische Anforderung, dies sollte durch das RZ gegeben sein, bankseitig ist eine ggf. erforderliche Parametrisierung zu dokumentieren.	Neue Richtlinie	IT-Organisation, Zahlungsverkehr
11.5	Überprüfung der dem Zahlungsdienstnutzer angebotenen Möglichkeiten zur Limitänderung	Das ist eine eher technische Anforderung, dies sollte durch das RZ gegeben sein, bankseitig ist eine ggf. erforderliche Parametrisierung zu dokumentieren.	Neue Richtlinie	IT-Organisation, Zahlungsverkehr
11.6	Überprüfung der dem Zahlungsdienstnutzer angebotenen Kontrollmöglichkeiten in Bezug auf Betrugsfälle	Das ist eine eher technische Anforderung, dies sollte durch das RZ gegeben sein, bankseitig ist eine ggf. erforderliche Parametrisierung zu dokumentieren.	Neue Richtlinie	IT-Organisation, Zahlungsverkehr
11.7	Überprüfung der dem Zahlungsdienstnutzer angebotenen Informationen zu Sicherheitsverfahren	Hierzu sollte ein entsprechender Prozess in der neuen Richtlinie hinterlegt werden (zeitnahe Information der Zahlungsdienstnutze über Aktualisierungen der Sicherheitsverfahren).	Neue Richtlinie	IT-Organisation, Zahlungsverkehr
11.8	Überprüfung der dem Zahlungsdienstnutzer angebotenen Kontaktinformationen und -möglichkeiten	Hierzu sollte ein entsprechender Prozess in der neuen Richtlinie hinterlegt werden (Unterstützung der Zahlungsdienstnutzer in Bezug auf alle Fragen, Unterstützungsanfragen, Benachrichtigungen über Unregelmäßigkeiten, sicherheitsrelevante Frage hinsichtlich Zahlungsdienst).	Neue Richtlinie	IT-Organisation, Zahlungsverkehr

3 Überblick wesentlicher Anpassungsbedarfe für Informationssicherheitsbeauftragte in Verbindung mit betroffenen Fachabteilungen

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
3.2	Überprüfung der Festlegung – der Prozessverantwortlichen der Fachbereiche im Sinne Informationseigentümer der Informationen/ Eigentümer Informationsrisiken – sowie der Verantwortlichen für das operative Informationsrisikomanagement	Erweiterung um Informationsrisiken. Dies sollte in der Informationssicherheitsleitlinie und im Informationsrisikomanagementprozess ergänzt werden. In der Vorgehensweise ergeben sich jedoch keine Änderungen.	Informationssicherheitsleitlinie, Informationsrisikomanagement	Informationssicherheits-beauftragter (organsatorische Grundlagen), Fachabteilung in Abstimmung mit Informationssicherheitsbeauftragter (Umsetzung)
3.3	– Überprüfung der dem Informationsverbund zugrunde gelegten Prozesse (Geschäfts- und Unterstützungsprozesse, IT-Prozesse) – Überprüfung, ob bei den Abhängigkeiten und Schnittstellen die Vernetzung des Informationsverbundes mit Dritten berücksichtigt wurde	Die Hinweise in den Erläuterungen sind in die Regelungen zum Informationsrisikomanagement-prozess aufzunehmen. Änderungen in der Vorgehensweise sollten sich nicht ergeben, im Regelfall erfolgt der Informationsrisikomanagement-prozess bereits wie dargestellt.	Informationsrisikomanagement	Informationssicherheits-beauftragter (organsatorische Grundlagen), Fachabteilung in Abstimmung mit Informationssicherheitsbeauftragter (Umsetzung)
3.4	– Sicherstellung, dass der Schutzbedarf der Geschäftsprozesse durch die Prozessverantwortlichen der Fachbereiche ermittelt wird und dies auch entsprechend dokumentiert wird	Grundsätzlich handelt es sich hierbei nicht um eine neue Anforderung. Konkretisiert ist jedoch, dass der Informationseigentümer die Ermittlung des Schutzbedarfs verantwortet. Dieses ist im Informationsrisikomanagementprozess entsprechend festzulegen.	Informationsrisikomanagement	Informationssicherheits-beauftragter (organsatorische Grundlagen), Fachabteilung in Abstimmung mit Informationssicherheitsbeauftragter (Umsetzung)

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
3.5	Überprüfung, dass eine vollumfängliche Plausibilitätsprüfung der Schutzbedarfsfeststellung durch Verantwortliche für das Informationsrisikomanagement durchgeführt wird.	Gem. Tz. 3.4 erfolgt die Bewertung des Schutzbedarfs durch den Informationseigentümer. Um eine korrekte Bewertung zu gewährleisten ist eine Überprüfung der Bewertung inkl. der Dokumentation durch den ISB zu vorzunehmen (Abgleich Schutzniveau - Schutzbedarf). Dieses ist im Informationsrisikomanagementprozess entsprechend festzulegen.	Informationsrisiko management	Informationssicherheits-beauftragter (organsatorische Grundlagen), Informations-risikomanagement (Umsetzung)
3.7	Überprüfung, ob regelmäßig ein Vergleich der Soll-Maßnahmen mit umgesetzten Maßnahmen erfolgt (Soll-Ist-Abgleich)	In weiten Teilen lediglich Anpassung der Formulierung. Der letzte Satz der Erläuterungen sollte in die Regelungen zum Informationsrisiko-managementprozess ergänzt werden.	Informationsrisiko management	Informationssicherheits-beauftragter (organsatorische Grundlagen), Fachabteilung in Abstimmung mit Informations-sicherheitsbeauftragter (Umsetzung)
3.9	Überprüfung der Methodik zur Risikoanalyse.	In den aktuellen BAIT wird klar gestellt dass das Informationsrisikomanagement die Risikoanalyse nicht selbst durchführt, sondern "lediglich" koordiniert und überwacht. Dieses ist im Informationsrisiko-managementprozess entsprechend festzulegen. Der Rest dieser neuen Tz. ist in dem vorherigen Stand der BAIT an anderen Stellen bereits enthalten gewesen.	Informationsrisiko management	Informationssicherheits-beauftragter
3.10	Überprüfung, inwieweit ausreichende Prozesse zur Erhebung und Bewertung der Bedrohungslage sowie der Ableitung geeigneter Maßnahmen implementiert wurden	Dieser Passus ist neu in die BAIT aufgenommen, dieses sollte in die Informationssicherheitsleitlinie (kurz) dargestellt werden. In den Regelungen für die IT-Organisation sollte dies konkretisiert werden.	Regelungen für IT-Organisation/ operativen IT-Betrieb o.ä.	Informationssicherheits-beauftragter

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
4.2	Überprüfung der Inhalte der Informationssicherheitsleitlinie (mit Blick auf die erweiterten BAIT-Anforderungen)	Veränderungsanforderung bei wesentlichen Veränderungen ist zu definieren. Zudem sollte in der bestehenden Informationssicherheitsleitlinie überprüft werden, ob die in den Erläuterungen der BaFin aufgeführten Inhalte in dieser bereits angemessen berücksichtigt sind.	Informationssicherheitsleitlinie	Informationssicherheits-beauftragter
4.7	Abgrenzung der Begriffe und Festlegung von eindeutigen Kriterien: – Informationssicherheitsvorfall – sicherheitsrelevantes Ereignis (im Sinne der operativen Informationssicherheit) – ungeplante Abweichung vom Regelbetrieb (im Sinne von „Störung“)	In den Regelungen zu den Informationssicherheits-vorfällen ist zu ergänzen, dass diese zeitnah analysiert und daraus ggf. Maßnahmen abgeleitet werden. Zudem sind die Begriffe "Informations-sicherheitsvorfall", "sicherheitsrelevantes Ereignis" und "ungeplante Abweichung vom Regelbetrieb" voneinander abzugrenzen. Hierbei ist zu berücksichtigen, dass der Begriff "sicherheits-relevantes Ereignis" neu ist. Siehe Inhalte der neuen BAIT (ist dargestellt)	Informationssicherheitsvorfälle	IT-Organisation in Abstimmung mit Informationssicherheits-beauftragter
4.8	Erstellung einer Richtlinie zum Testen und Überprüfen für die IT in der Bank	Neue Anforderung der BAIT. Es ist eine entsprechende Richlinie in der Bank mit den in den Erläuterungen der BaFin dargestellten Inhalten zu erstellen.	Neue Richtlinie	IT-Organisation in Abstimmung mit Informationssicherheits-beauftragter
4.9	Festlegen eines kontinuierlichen Sensibilisierungs- und Schulungsprogramms für Informationssicherheit	Neue Anforderung der BAIT. Es sollte ein entsprechendes Kapitel in die Regelungen zum Informationsrisikomanagement ergänzt werden.	Informationsrisiko management	Informationssicherheits-beauftragter

4 Überblick wesentlicher Anpassungsbedarfe für Informationssicherheitsbeauftragter und Notfallbeauftragten

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
3.11		Der Hinweis in den Erläuterungen sollte in die Regelungen zur Berichterstattung zu den Informationsrisiken sowie den Bericht des ISB ergänzt werden. Im Regelfall sollten externe potenzielle Bedrohungen bereits in den Risikoanalysen im Informationsrisikomanagementprozess ausreichend berücksichtigt sein.	Informationsrisiko-management, Bericht des ISB	Informationssicherheits-beauftragter
10.1	– Überprüfung der Notfallkonzeption der Bank gemäß MaRisk AT 7.3 neu – Berücksichtigung der IT-Dienstleister im Notfallmanagement.	Dieses Kapitel ist komplett neu in den BAIT, basiert jedoch auf den bekannten Anforderungen des AT 7.3 MaRisk und konkretisiert diese. In den Ausführungen zu den Tz. wird auf die Änderungen zu den bestehenden dokumentierten Regelungen nach Auffassung der DZ CP eingegangen. Bankseitig sollte das bestehende Notfallmanagement überprüft werden, ob die in den folgenden Tz. aufgeführten Regelungen / Prozesse bereits enthalten / abgedeckt sind.	Notfall-management	Notfallbeauftragter in Abstimmung mit Informationssicherheits-beauftragten

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
10.2	Überprüfung, dass Ziele und Rahmenbedingungen für das IT-Notfallmanagement festgelegt wurden	Erweiterung ders Notfallmanagement auf ein IT-Notfallmanagement. D.h. im Notfallmanagement sind nicht mehr "nur" die zeitkritischen Aktivitäten und Prozesse zu berücksichtigen sondern auch die hierfür erforderlichen IT-Systeme (Anwendungen, Systeme, Infrastruktur). Diese sind insofern - neben einer Anpassung der Regelungen für das Notfallmanagement - ebenfalls in das Notfallmanagement aufzunehmen. Die Anforderung ist nicht grundsätzlich neu, häufig sind jedoch noch nicht sämtliche IT-Systeme entsprechend berücksichtigt.	Notfall-management	Notfallbeauftragter in Abstimmung mit Informationssicherheits-beauftragten
10.3	– Überprüfung der Ermittlung der Verfügbarkeitsanforderungen über Auswirkungs- und Risikoanalysen – Überprüfung der IT-Notfallpläne bzw. Abgleich der Notfallpläne mit den IT-Notfallplänen der IT-Dienstleister	Siehe Tz. 10.2, an dieser Stelle ist die Anforderung definiert, dass für die zeitkritische Aktivitäten und Prozesse unterstützende IT entsprechende IT-Notfallpläne zu erstellen sind. Dies ist entsprechend im Notfallmanagement zu regeln.	Notfall-management	Notfallbeauftragter in Abstimmung mit Informationssicherheits-beauftragten

Text-ziffer	Handlungsbedarf gem. Checkliste des BVR	Anpassungsbedarf	Anzupassende Organisations-unterlagen	Umzusetzen durch …
10.4	Überprüfung, ob jährlich ausreichende IT-Notfalltests durchgeführt werden bzw. geeignete Nachweise vom IT-Dienstleister beigebracht werden	Hier ist eine Verschärfung der bisherigen Vorgehensweise enthalten: IT-Notfallpläne sind durch mindestens jährliche IT-Notfalltests zu überprüfen (bisher mehrjähriger Notfalltestplan). Zudem wird eine vollständige Abdeckung (unter Berücksichtigung von Abhängigkeiten, Systemverbünden etc.) gefordert. Dies ist im Notfallmanagement bei der Definition der IT-Notfalltests zu berücksichtigen. (Die Notfalltests müssen IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, vollständig abdecken. Abhängigkeiten zwischen IT-Systemen bzw. von gemeinsam genutzten IT-Systemen sind angemessen zu berücksichtigen. Hierfür ist ein IT-Testkonzept zu erstellen.)	Notfall-management	Notfallbeauftragter in Abstimmung mit Informationssicherheits-beauftragten
10.5	Überprüfung, dass ein Nachweis seitens des IT-Dienstleisters vorliegt	Neue Anforderung, nach Auffassung der DZ CP für die Banken, die neben der Fiducia, kein weiteres RZ (insbesondere kein eigenes RZ) nutzen, nicht von Bedeutung.	Notfall-management	Notfallbeauftragter in Abstimmung mit Informationssicherheits-beauftragten